

NKF Client News

2. DEZEMBER 2020

Revidiertes Bundesgesetz über den Datenschutz

Am 25. September 2020 haben die eidgenössischen Räte nach über zwei Jahren parlamentarischer Verhandlung das revidierte Datenschutzgesetz (DSG) verabschiedet. Trotz Totalrevision des Gesetzes bleiben die Grundprinzipien der Datenbearbeitung unverändert. Somit müssen auch nach der Revision die datenschutzrechtlichen Grundsätze (insbesondere Transparenz, Zweckbindung, Verhältnismässigkeit und Datensicherheit) eingehalten werden. Bei Beachtung dieser Grundsätze und sofern die Datenbearbeitung zu keiner Persönlichkeitsverletzung führt, gilt die Datenbearbeitung weiterhin, wie nach geltendem Recht, grundsätzlich als rechtmässig. Das heisst, eine Rechtfertigung der Bearbeitung durch Einwilligung, gesetzliche Grundlage oder überwiegendes privates oder öffentliches Interesse muss vor der Bearbeitung weiterhin nicht benannt werden. In dieser Hinsicht weicht das revidierte Gesetz mithin nach wie vor von der Datenschutz-Grundverordnung der EU (DSGVO) ab.

Dennoch ändert sich einiges unter dem revidierten DSG bzw. werden diverse Punkte an die DSGVO angepasst: Personendaten juristischer Personen sind nicht länger erfasst, Informationspflichten des Verantwortlichen werden erweitert, gewisse Datenschutz-Governance Pflichten werden neu eingeführt (bspw. Datenbearbeitungsverzeichnis, Datenschutz-Folgenabschätzung, Meldepflicht bei Datenschutzverletzungen, optionaler Datenschutzberater). Das revidierte DSG enthält auch einen verschärften Bussenkatalog und erweiterte Befugnisse des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). Bei Verletzungen der Vorschriften des revidierten DSG können die verantwortlichen Personen im Unternehmen persönlich mit Bussen bis maximal CHF 250'000.- bestraft werden.

Vor diesem Hintergrund hat das NKF-Datenschutz-Team die nachfolgende Compliance-Checkliste erarbeitet, welche Ihnen hilft, den Handlungsbedarf für die Umsetzung der neuen Datenschutzvorschriften in Ihrem Unternehmen besser abschätzen zu können. Mit einem Inkrafttreten ist nicht vor 2022 zu rechnen. Da das Gesetz aber (mit wenigen Ausnahmen) keine Übergangsfristen vorsieht, müssen die Unternehmen die notwendigen Vorkehrungen bis zum Inkrafttreten des revidierten Gesetzes getroffen haben. Bei Fragen stehen Ihnen die unten aufgeführten Autoren gerne zur Verfügung.

Thema	Artikel im revDSG	Kriterien	Was ist neu?
Geltungsbereich <i>Ist Ihr Unternehmen betroffen?</i>	Art. 2, 3	<input type="checkbox"/> Bearbeitung von Personendaten in der Schweiz <input type="checkbox"/> Bearbeitung von Personendaten ausserhalb der Schweiz, aber mit Wirkung in der Schweiz	Territorialer Geltungsbereich: "Auswirkungen" der Datenbearbeitung in der Schweiz lösen die Anwendbarkeit des revidierten DSG aus.
Daten <i>Welche Art von Daten sind betroffen?</i>	Art. 5	<input type="checkbox"/> Personendaten (alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen) <input type="checkbox"/> Besonders schützenswerte Personendaten (Daten über religiöse, ideologische, politische, gewerkschaftliche Ansichten oder Aktivitäten; Gesundheit; Intimsphäre; Rasse)	Daten von juristischen Personen sind nicht länger durch das revidierte DSG geschützt. Genetische Daten und biometrische Daten (die eine natürliche Person eindeutig identifizieren) sind neu explizit in

Thema	Artikel im revDSG	Kriterien	Was ist neu?
		oder ethnische Herkunft; genetische Daten; biometrische Daten; Daten über Verwaltungs- oder Strafverfahren und Sanktionen; Daten über Massnahmen der sozialen Sicherheit)	der Definition der besonders schützenswerten Daten aufgezählt. Die bisherige Pflicht zur Registrierung von Datensammlungen entfällt.
Profiling <i>Führen Sie ein Profiling durch?</i>	Art. 5, 6	<input type="checkbox"/> Profiling: automatisierte Bearbeitung personenbezogener Daten zur Beurteilung bestimmter persönlicher Aspekte einer natürlichen Person <input type="checkbox"/> Profiling mit hohem Risiko: Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person darstellt	Profiling ist vergleichbar mit dem "Persönlichkeitsprofil" gemäss geltendem Recht. Für ein Profiling mit hohem Risiko für die Persönlichkeit der betroffenen Person gelten dieselben qualifizierten Anforderungen an die Datenbearbeitung wie für "besonders schützenswerte Personendaten". Das bedeutet insbesondere, dass, sofern eine Einwilligung der betroffenen Person in die Bearbeitung erforderlich ist, diese ausdrücklich erfolgen muss.
Datensicherheit <i>Sind Ihre Daten sicher?</i>	Art. 7, 8	Der Verantwortliche und der Auftragsbearbeiter müssen die Datensicherheit durch angemessene technische und organisatorische Massnahmen gewährleisten: <input type="checkbox"/> Angemessene technische und organisatorische Massnahmen (sog. TOMs) <input type="checkbox"/> Umsetzung der Grundsätze "Privacy by Design" und "Privacy by Default"	Neu müssen technische und organisatorische Massnahmen für die Datensicherheit bereits bei der Planung eines Bearbeitungsvorgangs (Privacy by Design) und bei der Programmierung/beim Entwurf der Grundeinstellungen (Privacy by Default) berücksichtigt werden.
Auftragsbearbeitung <i>Werden die Daten von einem Auftragsbearbeiter bearbeitet?</i>	Art. 9	<input type="checkbox"/> Übertragung der Bearbeitung von personenbezogenen Daten an einen Auftragsbearbeiter weiterhin möglich (ausser eine gesetzliche oder vertragliche Geheimhaltungspflicht verbietet dies) <input type="checkbox"/> Auftrags-Datenbearbeitungsvertrag muss sicherstellen, dass die Daten durch den Auftragsbearbeiter nur so bearbeitet werden, wie es der Verantwortliche selbst tun dürfte	Keine Änderungen: Wie nach geltendem Recht (Art. 10a) kann die Bearbeitung einem Auftragsbearbeiter übertragen werden, wenn der Verantwortliche sicherstellt, dass der Auftragsbearbeiter in der Lage ist, die Datensicherheit zu gewährleisten und, dass die Personendaten nur in der für den Verantwortlichen selbst zulässigen Weise bearbeitet werden.
Verantwortung <i>Wer ist innerhalb des Unternehmens für die Einhaltung des Datenschutzes verantwortlich?</i>	Art. 10	Für die Einhaltung der anwendbaren Datenschutzgesetze ist grundsätzlich der Verwaltungsrat zuständig, da er die Oberleitung einer Gesellschaft innehat. Er kann dies aber an die Geschäftsleitung oder einen betriebsinternen oder -externen Datenschutzverantwortlichen delegieren (welcher unabhängig von der Geschäftsleitung agieren können muss): <input type="checkbox"/> Hat das Unternehmen einen Datenschutzberater ernannt? <input type="checkbox"/> Wurde eine Person innerhalb des Managements bestimmt, welche die Einhaltung des DSG unterstützt? <input type="checkbox"/> Wurde eine Person in jeder jeweiligen lokalen Geschäftseinheit mit der Einhaltung des Datenschutzes beauftragt? <input type="checkbox"/> Ist die Unabhängigkeit des Datenschutzberaters sichergestellt und besteht ein klares Pflichtenheft?	Die Verantwortung für die Einhaltung des Datenschutzes verbleibt beim Verantwortlichen. Der interne Datenschutzverantwortliche wird neu als Datenschutzberater bezeichnet. Unternehmen können (müssen aber nicht) einen Datenschutzberater ernennen, der als Kontaktstelle für die betroffenen Personen und für die in der Schweiz für Datenschutzfragen zuständigen Datenschutzbehörden dient.
Verzeichnis <i>Müssen Sie ein Verzeichnis der Bearbeitungstätigkeiten führen?</i>	Art. 12	<input type="checkbox"/> Auflistung aller Bearbeitungstätigkeiten, inklusive des Bearbeitungszwecks, der Datenkategorien, einer Beschreibung der Massnahmen zur Gewährleistung der Datensicherheit, der Angabe der Staaten bei	Neue Pflicht für den Verantwortlichen und den Auftragsbearbeiter.

Thema	Artikel im revDSG	Kriterien	Was ist neu?
		<p>Auslandtransfers von Daten sowie der entsprechenden Garantien etc.</p> <p><input type="checkbox"/> Data Retention Schedule, welcher die Aufbewahrungsdauer der einzelnen Datenkategorien auflistet</p>	<p>Der Bundesrat kann Ausnahmen für Unternehmen mit weniger als 250 Mitarbeiter vorsehen, falls deren Datenbearbeitung ein geringes Risiko von Verletzungen der Persönlichkeit der betroffenen Personen mit sich bringt.</p>
<p>Vertreter <i>Wer muss einen Vertreter ernennen?</i></p>	Art. 14	<p>Verantwortliche mit Wohnsitz/Sitz ausserhalb der Schweiz benennen einen Vertreter in der Schweiz, wenn sie Personendaten von Personen in der Schweiz bearbeiten und die Datenbearbeitung die folgenden Voraussetzungen erfüllt (kumulativ):</p> <p><input type="checkbox"/> die Datenbearbeitung steht im Zusammenhang mit dem Anbieten von Waren oder Dienstleistungen oder der Beobachtung des Verhaltens von Personen in der Schweiz;</p> <p><input type="checkbox"/> die Datenbearbeitung erfolgt umfassend und regelmässig und bringt ein hohes Risiko für die Persönlichkeit der betroffenen Personen mit sich</p>	<p>Neue Pflicht für den Verantwortlichen mit Sitz/Wohnsitz im Ausland.</p>
<p>Übermittlung von Daten <i>Was gilt, wenn Personendaten ins Ausland bekanntgegeben werden?</i></p>	Art. 16	<p>Rechtliche Grundlagen für den Datentransfer ins Ausland:</p> <p><input type="checkbox"/> Vom Bundesrat anerkannt, dass im betreffenden Staat ein gleichwertiges Datenschutzniveau besteht; sonst</p> <p><input type="checkbox"/> gruppeninterne Datenübertragungsvereinbarungen/Datenschutzvorschriften (sogenannte Binding Corporate Rules)</p> <p><input type="checkbox"/> Anerkannte Standardvertragsklauseln (EU-Musterklauseln oder EDÖB-Mustervertrag)</p>	<p>Keine Änderungen der Grundprinzipien für Datenexporte. Neu erlässt der Bundesrat Angemessenheitsentscheide über das Datenschutzniveau anderer Staaten (bisherige "Staatenliste" des EDÖB entfällt). Die Notifikationspflicht bei Verwendung von genehmigten Standardvertragsklauseln entfällt. Hinweis: Nach dem Schrems-II-Entscheid des EuGH ist der Privacy Shield gemäss EDÖB keine ausreichende Rechtsgrundlage mehr für den Datentransfer in die USA (→ andere Datenschutzmassnahmen umsetzen). Gemäss EDÖB muss für jeden Drittstaat geprüft werden, ob das lokale öffentliche Recht die verwendeten vertraglichen Regelungen (z.B. Standardvertragsklauseln) respektiert.</p>
<p>Informationspflicht <i>Welche Massnahmen müssen Sie treffen?</i></p>	Art. 19	<p><input type="checkbox"/> Datenschutzbestimmungen, die der betroffenen Person alle Informationen zur Verfügung stellen, die sie benötigt, um ihre Rechte gemäss dem DSG geltend zu machen; mindestens mitzuteilen sind: (i) die Identität und die Kontaktdaten des Verantwortlichen, (ii) der Bearbeitungszweck, (iii) gegebenenfalls die Empfänger denen Personendaten bekanntgegeben werden, (iv) bei Bekanntgabe ins Ausland den Staat und gegebenenfalls die Garantien (bspw. Binding Corporate Rules), (v) gegebenenfalls die Kategorien der bearbeiteten Personendaten</p> <p><input type="checkbox"/> Cookie-Richtlinie (inkl. Zustimmungspflicht für nicht-technische Cookies)</p>	<p>Im Vergleich zum geltenden Recht bestehen konkrete und erweiterte Informationspflichten mit Bezug auf die Bearbeitung aller Arten von Personendaten.</p>
<p>Datenschutz-Folgenabschätzung (DSFA) <i>Wann müssen Sie eine DSFA durchführen?</i></p>	Art. 22	<p>Wenn die beabsichtigte Bearbeitung zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führen kann, muss eine DSFA durchgeführt werden:</p> <p><input type="checkbox"/> Besteht eine Dokumentation zur Durchführung einer DSFA (inkl. Methodik)?</p>	<p>Neue Pflicht für den Verantwortlichen. Ein hohes Risiko ist insbesondere bei der Verwendung neuer Technologien oder bei umfangreicher Bearbeitung von besonders</p>

Thema	Artikel im revDSG	Kriterien	Was ist neu?
		<input type="checkbox"/> Ist ein Register von durchgeführten DSFA vorhanden?	schützenswerten Personendaten gegeben. Die DSFA muss eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen zum Schutz der Persönlichkeit und der Grundrechte enthalten.
Verletzung der Datensicherheit <i>Haben Sie eine Meldepflicht?</i>	Art. 24	Verfahren zur Benachrichtigung des EDÖB im Falle einer Verletzung der Datensicherheit (" <u>so rasch als möglich</u> "): <input type="checkbox"/> Reaktions- und Benachrichtigungsplan (inkl. Benachrichtigungsformular) für mögliche zukünftige Fälle von Verletzungen der Datensicherheit <input type="checkbox"/> Ist ein Register vorhanden, in welchem Verletzungen der Datensicherheit dokumentiert werden?	Neue Meldepflicht für den Verantwortlichen, sofern die Verletzung der Datensicherheit voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt. Die betroffene Person muss informiert werden, wenn es zu ihrem Schutz erforderlich ist oder der EDÖB es verlangt.
Rechte der betroffenen Person <i>Welche Rechte müssen Sie beachten?</i>	Art. 25, 32	Vorsehen interner Verfahren, um auf folgende Rechte der betroffenen Personen zu reagieren: <input type="checkbox"/> Auskunftsrechte <input type="checkbox"/> Berichtigung von Daten <input type="checkbox"/> Löschung von Daten <input type="checkbox"/> Entscheidungen auf der Grundlage automatisierter Bearbeitung	Die Rechte der betroffenen Personen werden unter dem revidierten DSGVO leicht erweitert bzw. spezifiziert. Dies gilt insbesondere für die Rechte betroffener Person in Zusammenhang mit Entscheidungen, welche ausschliesslich auf einer automatisierten Bearbeitung beruhen.
Recht auf Datenportabilität <i>Müssen Sie Daten an die betroffenen Personen herausgeben?</i>	Art. 28	<input type="checkbox"/> Auf Anfrage der betroffenen Person muss der Verantwortliche in der Lage sein, personenbezogene Daten in einem elektronischen Standardformat herauszugeben (sofern der Verantwortliche die Daten automatisiert bearbeitet und die Daten mit der Einwilligung der betroffenen Person oder in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages zwischen dem Verantwortlichen und der betroffenen Person bearbeitet werden)	Neue Pflicht für den Verantwortlichen. Die Daten sind grundsätzlich kostenlos herauszugeben, der Bundesrat kann aber Ausnahmen vorsehen, namentlich wenn der Aufwand unverhältnismässig ist.
Neue Befugnisse des EDÖB/Sanktionen <i>Welche Massnahmen gewährt ein Unternehmen bei einem Verstoß gegen das DSG?</i>	Art. 51 ff.	Nach dem revidierten DSGVO kann der EDÖB (von Amtes wegen oder nach Meldung) die Datenbearbeitungstätigkeiten untersuchen und bei Verstössen administrative Massnahmen anordnen (bspw. Einstellung der Bearbeitung). Bei Verletzung von DSGVO-Pflichten sind die Bussen persönlich (bis zu CHF 250'000). Entsprechend sollte geprüft werden: <input type="checkbox"/> Umfang der D&O-Versicherung <input type="checkbox"/> Spezifische Datenschutzversicherung (Neuabschluss oder Prüfung Umfang)	Prüfen Sie den Versicherungsschutz auf Bussgelder für Datenschutz- und Sicherheitsverletzungen.

Diese Checkliste dient nur dazu, Ihnen einen kurzen Überblick über die wichtigsten Neuerungen des revidierten Datenschutzgesetzes zu verschaffen, soweit heute bekannt (Stand: November 2020). Sie dient nicht der rechtlichen Beratung.

Sollten Sie zu diesem Thema weitere Fragen und Anregungen haben, wenden Sie sich gerne an Ihren regulären NKF-Kontakt.

Autoren/Kontakt

Clara-Ann Gordon
Partner, Technology/Data Protection
clara-ann.gordon@nkf.ch

Dr. András Gurovits
Partner, Technology/Data Protection
andras.gurovits@nkf.ch

Janine Reudt-Demont
Counsel, Life Sciences/Healthcare
janine.reudt-demont@nkf.ch

Eric Neuenschwander
Associate, Technology/Data Protection
eric.neuenschwander@nkf.ch

Diese Publikation behandelt nicht zwingend jedes wichtige Thema und deckt nicht jeden Aspekt der Themen ab, mit denen sie sich beschäftigt. Sie dient nicht der rechtlichen oder sonstigen Beratung.

